Cyber Hygiene

Definition of Cyber Hygiene:
Cyber hygiene is the reference to a set of practices and steps that users of computers and other devices take to maintain system health and improve online security. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.

Why is Cyber Hygiene Important?
A system that is well-maintained is less likely to be vulnerable to cybersecurity risks. Security is perhaps the most important reason to incorporate a cyber hygiene routine. Hackers, identity thieves, advanced viruses, and intelligent malware are all part of the hostile threat landscape. While predicting threats can be challenging, preparing and preventing them becomes feasible with sound cyber hygiene practices.

The Impact of Bad Cyber Hygiene
Enterprises often have multiple elements in need of cyber hygiene. All hardware (computers, phones, connected devices), software programs, and online applications used should be included in a regular, ongoing maintenance program. Each of these systems have specific vulnerabilities that can lead to different problems. Some of these problems include:

- **Loss of Data**: Hard drives and online cloud storage that is not backed up or maintained is vulnerable to hacking, corruption, and other problems that could result in the loss of information.

- **Misplaced Data**: Poor cyber hygiene could mean losing data in other ways. The information may not be corrupted or gone for good, but with so many places to store data, misplacing files is becoming increasingly commonplace in the modern enterprise.

- **Security Breach:** There are constant and immediate threats to all enterprise data. Phishing, hackers, malware, spam, viruses, and a variety of other threats exist in the modern threat landscape, which is constantly in a state of flux.

- **Out of Date Software:** Software applications should be updated regularly, ensuring that the latest security patches and most current versions are in use across the enterprise – for all applications. Out of date software is more vulnerable to attacks and malware.

- **Older Security Software:** Antivirus software and other security software must be updated continuously to keep pace with the ever-changing threat landscape. Outdated security software – even software that has gone a few months without an update – can't protect the enterprise against the latest threats.

Good Cyber Hygiene
Here are a few strategies that everyone can practice to promote good cyber hygiene.

- **Update Regularly:** Installing updates across devices, applications, and operating systems on a regular basis is an integral step to achieving strong cyber hygiene. Though it's easy to ignore updates when you need to meet a deadline or help a customer, failure to keep your devices updated can drastically simplify the process for cybercriminals seeking to corrupt your device. One of the most effective—and easiest—ways to avoid that tendency is to simply add patching and updating to your work schedule.

- **Strong Access Management:** a simple but very effective cyber hygiene best practice. You should be using strong passwords and two-factor authentication across all devices and accounts – especially on devices and applications that are used to access sensitive business information. Strong passwords augmented with two-factor authentication is even better, ensuring that only authorized people can access business-critical systems and sensitive data.

- **Practice Safe Email Use:** The most popular attack vector still being leveraged by cybercriminals today is email. Because email is everywhere, it remains the easiest way to distribute malware to unsuspecting users. Educate yourself and users to never click on a link or attachment from an unknown sender. And even if an email seems to come from a trusted source, be sure to look closely at the email address or website URL they refer you to. Often, names or URLs will have misspellings, which indicate an attack. Unexpected requests are ALWAYS suspect and may warrant directly contacting the sender to not only verify the request, but if it is legitimate, to also suggest that they use a different process besides distributing unannounced attachments and links.

- **Install Anti-Malware:** While anti-malware software cannot stop unknown attacks, most attacks and exploits reuse attacks that have been previously successful. Installing anti-malware/anti-virus software across all your devices and networks provides protection in the event of a successful phishing scam or an attempt to exploit a known vulnerability.

- **Don't Overshare on Social Networking Sites:** If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

5 ways to Improve Your Personal Cyber Hygiene

Close	Check	Enable	Update	Use
Close Dormant or Unused accounts	Check what apps connect to your account and what assess and if the type of access is necessary.	Enable 2FA for all your accounts to prevent unauthorized access.	Update your Mobile apps	Use a sperate email account for your social media accounts

Lastly, with our data being the new oil for marketers and hackers, cybersecurity is no longer just the sole responsibility of IT and the security teams. As employees interact with and rely on technology every day, we all play an integral role in the security of our personal and professional cyber hygiene practices. As the old Homeland Security adage goes "see something say something ".